



Rules and Responsibilities for Accessing, Using, Sharing, and Protecting NORS and DIRS Information

NETWORK OUTAGE REPORTING SYSTEM (NORS) AND
DISASTER INFORMATION REPORTING SYSTEM (DIRS)
TRAINING MATERIALS
[MONTH], 2022

Overview

- The Federal Communications Commission (FCC) has granted [agency name] a limited number of user accounts to access and for use of the FCC's Network Outage Reporting System (NORS) and Disaster Information Reporting System (DIRS) filings and the necessary information safeguards.
- These filings contain confidential information and business contact information, which the FCC considers to be personally identifying information (PII). The filings are supplied to the FCC by the nation's service providers to provide timely information on network outages and infrastructure status.
- This training program covers access to, use of, and compliance with information safeguards so that [agency name] can further its public safety mission while taking steps to prevent improper disclosure and misuse.
- As an employee designated by your agency to receive a NORS/DIRS user account, you are required to review these training materials prior to using the account and then at least annually thereafter to maintain access.

Agency Coordinator

- Questions or concerns related to this training or terms of the sharing program should be directed to your agency's coordinator:
 - [agency coordinator name]
 - [job title]
 - [phone number and/or email address]
- Your agency coordinator is your initial point of contact for all matters related to this program. Your coordinator:
 - manages distribution and reassignment of NORS/DIRS user accounts, and internal sharing of NORS/DIRS information.
 - coordinates the downstream sharing of NORS and DIRS filings with those outside your agency.
 - coordinates with the FCC to manage incidents (e.g., an unauthorized access incident) and any auditing requirements.

Agency Coordinator

- If you are a new user of NORS/DIRS, your agency coordinator will provide you with a user account to directly access filings, if you do not already have one.
 - The user account is unique to you; it is not to be shared with others under any circumstances.
 - Your authorization to use the account ends if you change roles or leave the agency; you must notify your agency coordinator so that your user account can be reassigned.
- Under certain circumstances—upon request and when determined to be in the public interest—information regarding your access to NORS or DIRS filings (e.g., an audit log) may be released to a service provider whose filings you have accessed.

NORS and DIRS Filings

- The NORS/DIRS filings provide timely information on the status of network outages and infrastructure status as reported by service providers to the FCC.
- Your user account will give you read-only access to NORS and DIRS filings from September 30, 2022 onwards that describe events occurring at least partially in your state or territorial borders or federal jurisdiction.*
- Due to the nature of the reporting process, there is no guarantee that NORS and DIRS filings are accurate; they represent the best information as known to the service provider at the time of filing and are updated as additional information is discovered.
- There may be times when access to the NORS and DIRS systems is unavailable, e.g., due to planned or unplanned service and maintenance.

**States receive access to filings for events occurring in nearby Tribal territory land and Tribal territories receive access to filings on events in states surrounding their land.*

DIRS

What is DIRS?

- DIRS is a voluntary, web-based system through which the FCC collects operational status and restoration information from communications providers during major disasters and subsequent recovery efforts. DIRS is activated by the FCC on a local or regional basis when an emergency warrants it.

Purposes of DIRS:

- Supplies a single, coordinated, consistent process for communications providers to report their communications infrastructure status information during disasters.
- Provides situational awareness for state and federal agencies working on restoration:
 - Shows areas most affected.
 - Helps coordinate restoration efforts.
- Tracks the effectiveness of restoration efforts.
- Provides consistent information from companies in each segment of the communications sector.

DIRS Scope

DIRS collects status information on the following:

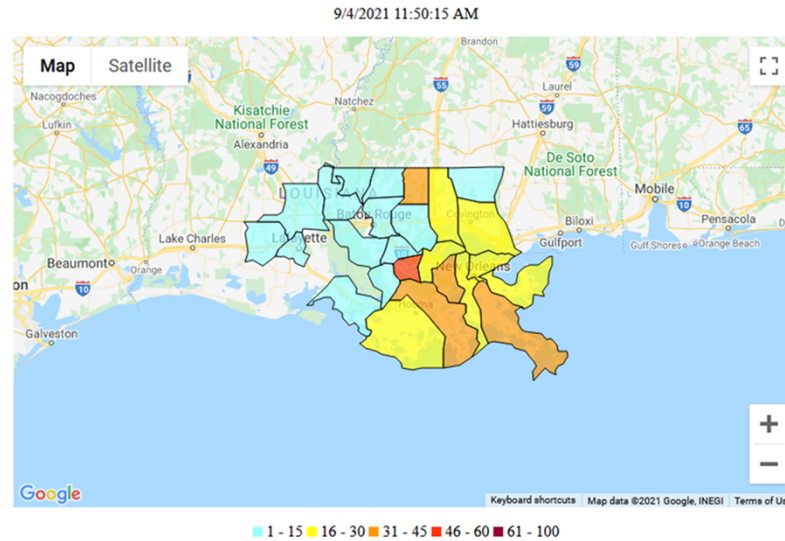
- PSAPs
- Major Equipment – Wireline, Cable
- Wireless Routing Assets
- Wireless Cell Sites by County
- Remote Aggregation Devices/Distribution
- Broadcast – AM, FM, TV Stations
- Cable Systems
- Satellite Earth/Ground Stations
- Contact information about the infrastructure

DIRS Reporting Process

1. FCC, in coordination with DHS (FEMA and CISA), determines which counties should be included in the activation area.
2. FCC activates DIRS and issues a public notice announcing DIRS activation.
3. DIRS team at the FCC sends DIRS activation notice to all communication providers, including broadcasters, that are signed up in DIRS.
4. DIRS data is due to be submitted by 10:00 AM ET the following morning after the activation and updated every day thereafter until DIRS is deactivated.
5. DIRS team gathers and analyzes the data, works with companies to resolve any reporting issues and then prepares a situation report with maps of the affected area showing the status of communications, which is sent to members of the Federal Emergency Support Function #2 to assist disaster recovery effort. The information is consolidated but may still contain company confidential information and PII.
6. A public report is generated and posted on the FCC website. This report excludes any confidential company information (e.g., information pertaining to a single report or specific communications facility is generalized or omitted)

Examples of Public DIRS Analysis

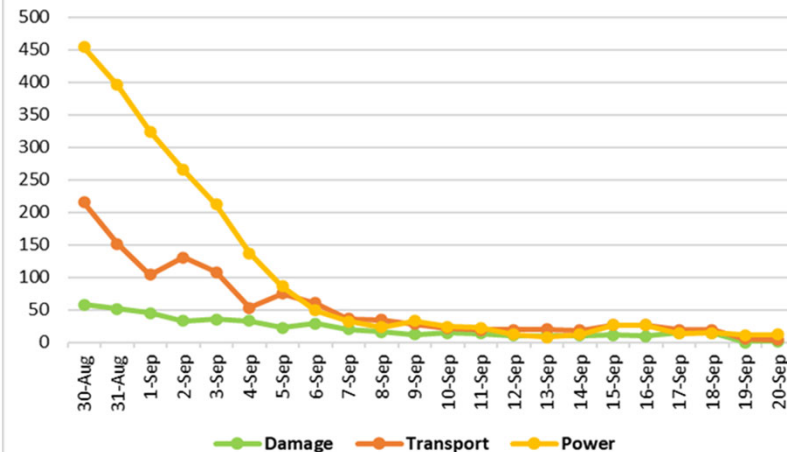
Percent Cell Sites Out-of-Service By County



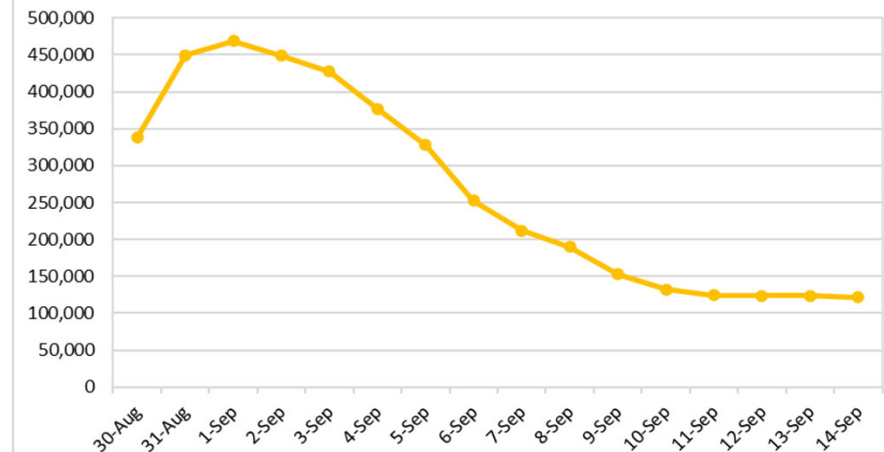
Number of PSAPs Affected in the Disaster Area by Date



Number of Cell Sites Out of Service by Cause in Disaster Area in LA by Date



Total Number of Wireline/Cable Users Affected in the DIRS Activation Areas



NORS

What is NORS?

- NORS is a mandatory, web-based system through which the FCC collects information on significant communications service disruptions that could affect homeland security, public health or safety, and the economic well-being of the nation.
- NORS allows the FCC to identify trends and monitor network performance.
- Covered communication providers (wireline, cable, satellite, submarine cable, wireless, interconnected VoIP and Signaling System 7 providers) are required to report network outages that last at least 30 minutes and satisfy other specific magnitude thresholds.

Purposes of NORS:

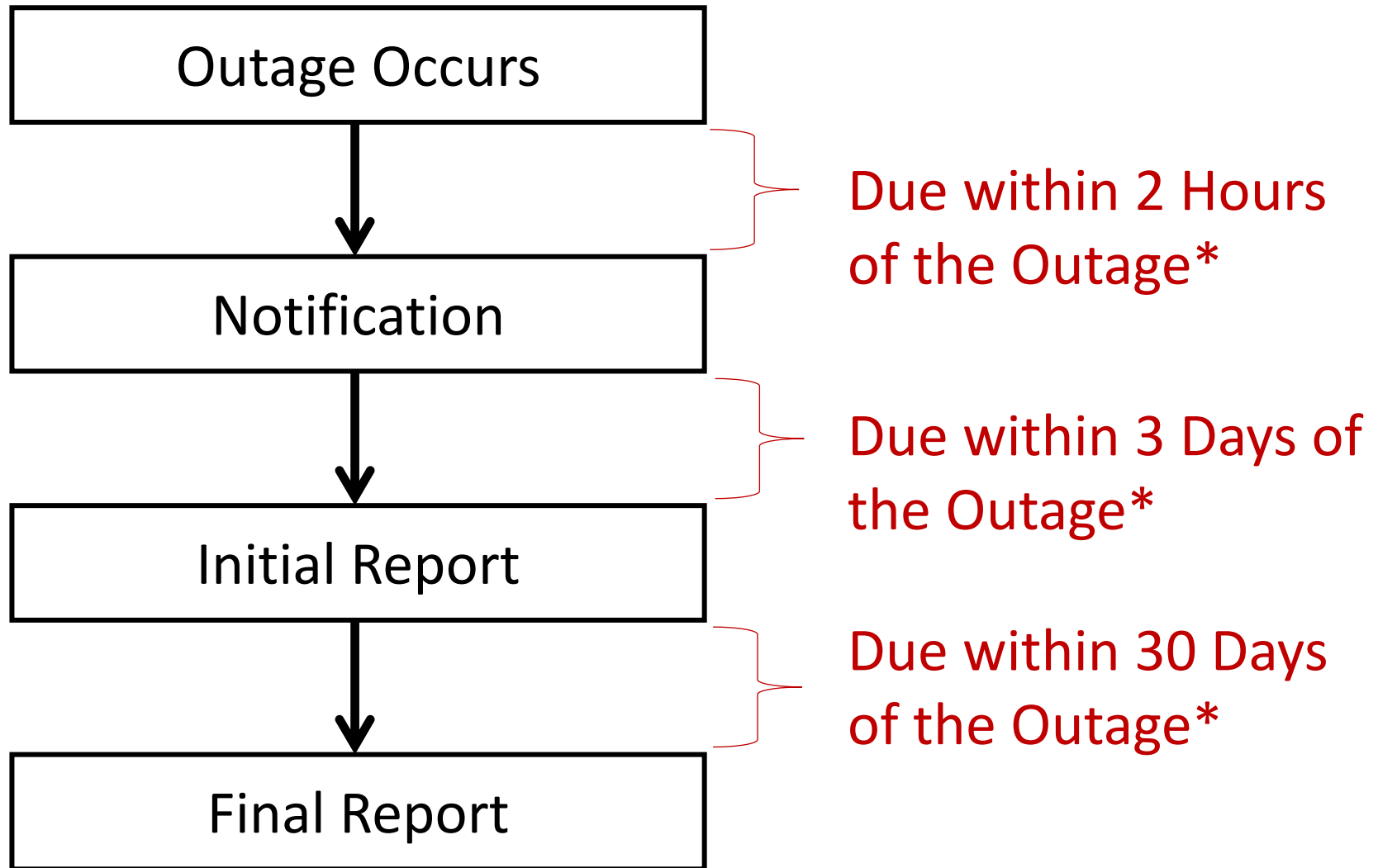
- Improve FCC awareness on major communications outage.
- Improve and informs the FCC on communications network reliability, security, and disaster recovery.

NORS Outage Reporting Thresholds

At least 30 minutes long and at least one of the following criterion is satisfied:

- VoIP
 - 900,000 User minutes
- Wireline
 - 900,000 User minutes
 - 90,000 Blocked calls
- Wireless
 - 900,000 User minutes
 - 90,000 Blocked calls
 - Mobile Switching Center outage
- Cable Telephony – 900,000 User minutes, 90,000 blocked calls
- Emergency Services - E911 – 900,000 User Minutes
- Infrastructure Failures
 - OC3 – 667 OC3 minutes
 - OC3 – Simplex greater than 4 days
- SS7 Failures
- Failures of Special Facilities
 - Airport
 - Other Special Facilities - (Military, Nuclear, etc.)
- Paging
- Satellite
- Submarine Cable

NORS Reporting Process and Timeline

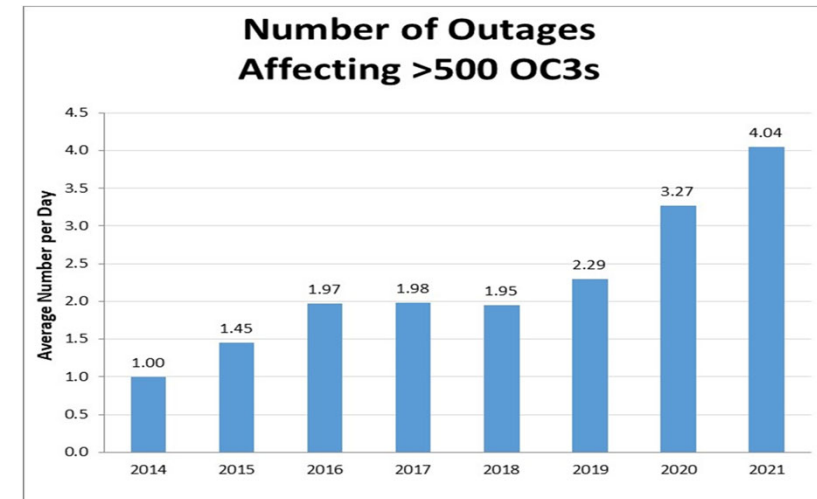
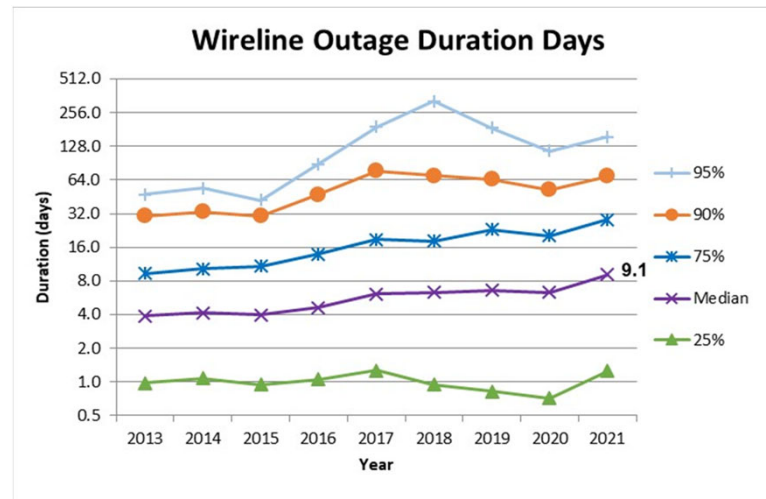
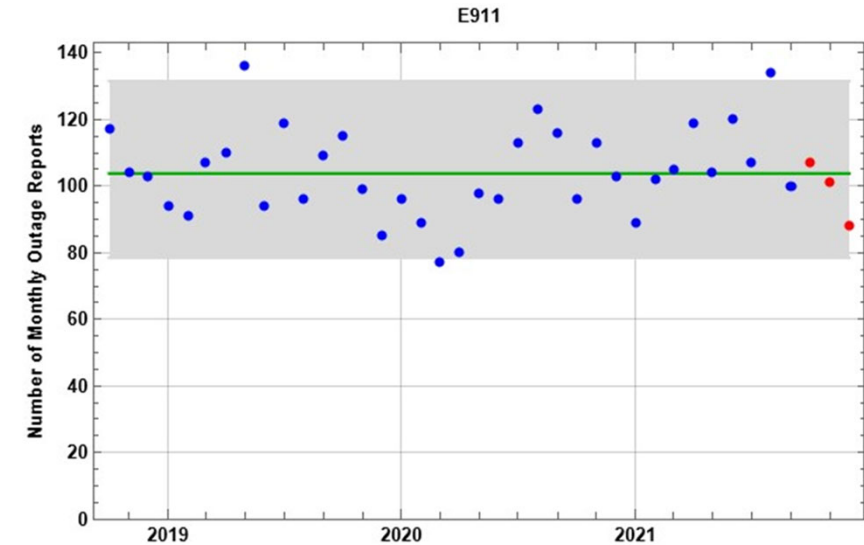
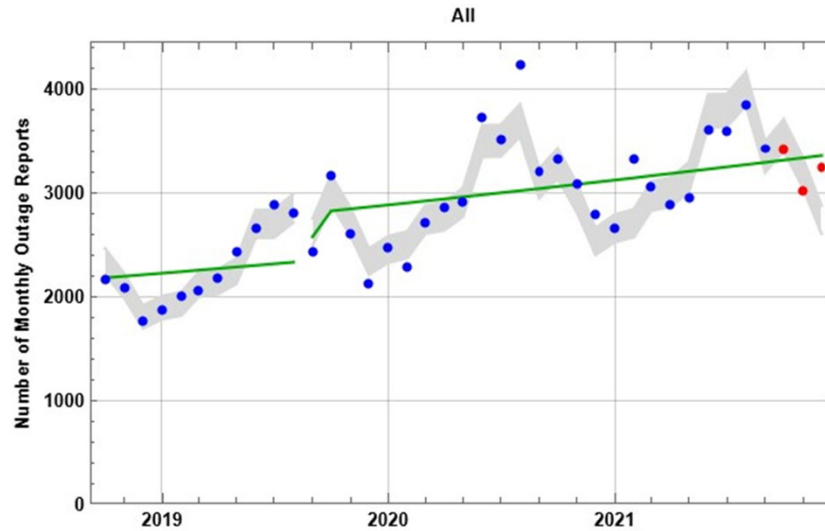


* Outages in VoIP networks have different reporting timeline requirements. Notifications must be filed within 240 minutes; Initial Reports within 24 hours; and Final Reports within 30 days.

Keys Contents of NORS Final Reports

- When outage occurred
- Description of event
- Duration of outage
- Location of the effects of the event
- Effects of the outage – number of customers affected
- Causes of the event
- Whether malicious or not
- Part of network involved
- Steps taken to prevent future occurrences
- CSRIC best practices related to an outage
- Contact information about the outage

Examples of NORS Aggregated Data



NORS/DIRS Confidential Information

- NORS and DIRS filings are confidential under Federal law due to national security and commercial competitiveness considerations.
- NORS and DIRS filings contain business contact information for each service provider, which the FCC treats as PII.
- “NORS/DIRS confidential information” refers to NORS/DIRS filings, in whole or part, and any confidential information derived from the filings.
- You may only use NORS/DIRS confidential information to carry out emergency management and first responder support functions that your agency is directly responsible for pursuant to its official duties (a “need to know” standard).
- Permitted uses of NORS/DIRS confidential information based on this “need to know” basis:
 - informing the public of danger, or preparing in advance for such danger, to avoid the loss of life and property.
 - assessing emergency notification options available in areas impacted by an outage or disaster and/or coordinating alternate methods of notification.
 - identifying trends and performing analyses designed to make long-term improvements in public safety outcomes.

NORS/DIRS Confidential Information

- You may not use NORS/DIRS Confidential Information for **any** non-emergency-related regulatory purposes, including, for example:
 - merger review.
 - consumer protection activities.
 - contract disputes involving service providers.
 - release of service provider competitive information.

Your agency's "need to know" for the filings is not based on any of these grounds/activities.

Sharing NORs/DIRS Confidential Information: Within Your Agency

You may share NORs/DIRS confidential information ***within your agency*** with other employees who have a “need to know,” i.e., who carry out official emergency management and first responder support functions that the agency is directly responsible for.

- Recipients within your agency with a “need to know” may include, e.g., decision makers and other supervisors in your chain of command.
- Those recipients may not further share or disclose NORs/DIRS confidential information.
- Contractors are *outside* your agency for the purposes of the sharing program. You may not share NORs/DIRS confidential information with contractors except as described next.

Sharing NORs/DIRS Confidential Information: Outside Your Agency

- You may share NORs/DIRS confidential information with any individual ***outside your agency***, including your agency's contractors, if your agency coordinator determines that the recipient has a "need to know."
- Other differences when sharing outside your agency:
 - Your agency coordinator is responsible for the "need to know" determination.
 - The "need to know" must pertain to a specific imminent or on-going public safety event (sharing for purposes of long-term trend analysis not permitted).
 - A log must be kept of all outside recipients with whom information is shared (your coordinator may maintain this log or ask you to do so).
 - Potential outside entities to share with:
 - PSAPs / 911 authorities
 - Local police agencies
 - First responders
 - Other local (city, county, etc.) public safety agencies
 - Your agency's contractors charged with restoration and recovery efforts

Sharing NORs/DIRS Confidential Information: Outside Your Agency

- Before sharing outside your agency, your agency must instruct downstream recipients to keep NORs and DIRS information they receive as confidential. Your agency must obtain a certification from downstream entities that they will treat the information as confidential, not disclose it absent a finding by the FCC that allows it to do so, report any unauthorized access, and securely destroy the information when the public safety event that warrants its access to the information has concluded.
 - A certification for your agency's use for this purpose is available on the FCC's website at [REDACTED].
- The downstream recipient may not further share NORs/DIRS confidential information and should not be asked to do so.

Sharing NORs/DIRS Aggregated Information: With the Public

- You may share **aggregated** NORs/DIRS information with any entity including the broader public.
 - “Aggregated NORs/DIRS information” refers to information from the NORs and DIRS filings of at least four service providers that has been aggregated and anonymized to avoid identifying any service providers by name or in substance.
 - In other words, you may not publicly release information that could allow the public or a service provider to deduce specific information that another service provider filed.
 - This information can be used, e.g., to keep the public informed of ongoing emergency and network outage situations, timelines for recovery, and geographic areas to avoid while disaster and emergency events are ongoing.

Sharing

- No other sharing or NORS/DIRS confidential information is permitted except as described in these slides.
- If you receive any requests to share filings, or information derived from filings, in ways you have not been authorized to do, please refer them promptly to your agency coordinator.
 - This includes any requests from third-parties based on your state's open records laws.
 - Your agency coordinator will work with the FCC to address such requests.

Notification/Reporting Obligations

- You must immediately report to your agency coordinator your knowledge of any of the following:
 - any request from a third party that you or your agency disclose NORS filings and DIRS filings pursuant to open records laws or any other legal authority.
 - any change in applicable rules or statutes that would affect the agency's ability to adhere to the protections described in this training.
 - any known or reasonably suspected unauthorized use or improper disclosure of NORS and DIRS information and any known or reasonably suspected breach of the protocol specified in the training program.
- Your agency coordinator will coordinate reporting these incidents to the FCC and/or affected service providers as appropriate.

Failure to Abide by the Program Rules

- Failure to abide by program rules will result in personal or agency termination of access to NORS and DIRS filings and potentially liability to service providers and third-parties as applicable under state and federal law.
- Participating agencies will be held responsible for inappropriate disclosures of NORS and DIRS information by the non-participating agencies with which they share it.
 - This kind of inappropriate disclosure could also result in termination of access to NORS and DIRS data.
- The FCC maintains auditing capabilities into NORS and DIRS that track which reports you access and when they are accessed.
 - Logs are used by FCC to maintain oversight and ensure accountability.
 - Logs may be made available to service providers upon request.

Conclusion

- Questions or concerns related to this training or terms of the sharing program should be addressed with your agency's coordinator:

[employee name]

[title]

[phone number and/or email address]

Your coordinator is your initial point of contact for all matters related to this program.

- While your agency coordinator should be able to answer your questions, you may also contact the FCC with questions or reporting under this program at NORS_DIRS_information_sharing@fcc.gov.



Questions?